IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: William Henry Yost

Examiner: Abedin, S.

Serial No: 10/089,506

Group Art Unit: 2136

Filed: August 9, 2002

Docket: RCA89826

For: SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Applicants appeal the status of Claims 1-7 as presented in response to the Office Action dated March 22, 2006, and finally rejected in the Office Actions dated August 22, 2006 and October 13, 2006 pursuant to the Notice of Appeal filed concurrently herewith and submit this appeal brief.

TABLE OF CONTENTS:

1. Real Party in Interest

2. Related Appeals and Interferences

3. Status of Claims

4. Status of Amendments

5. Summary of Claimed Subject Matter

6. Grounds of Rejection to be Reviewed on Appeal

7. Argument

A. Introduction

B. Whether Claim 1 is Unpatentable Under 35 U.S.C. §103(a) by SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 in view of Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998

B1. The Cited Combination of Stallings and StJohns Does Not Teach Or Suggest Converting The Shared Secret Into A Readable Password, As Recited In Claim 1

B2. The Cited Combination of Stallings and StJohns Would Change The Principle Of Operation Of Stallings, Thereby Making The Teachings of The Combination Not Sufficient To Render Claim 1 Prima Facie Obvious

B3. No Teaching, Suggestion, or Motivation Exists To Combine And/Or Modify Stallings And/Or StJohns To Produce The Invention Claimed In Claim 1

C. Conclusion

8. CLAIMS APPENDIX

9. RELATED EVIDENCE APPENDIX

10. RELATING PROCEEDINGS APPENDIX

1. Real Party in Interest

The real party in interest is THOMSON LICENSING S.A., the assignee of the entire right title and interest in and to the subject application by virtue of an assignment recorded with the Patent Office on March 28, 2002 at reel/frame 012800/0590.

2. Related Appeals and Interferences

None.

3. Status of Claims

Claims 1-7 are pending. Claims 1-7 stand rejected and are under appeal.

A copy of the Claims 1-7 is presented in Section 8 below.

4. Status of Amendments

An amendment under 37 CFR §1.111, mailed to the PTO on June 7, 2006 in response to the non-final Office Action dated March 22, 2006, was entered. An amendment under 37 C.F.R. §1.116, mailed to the PTO on September 26, 2006 in response to the final Office Action dated August 22, 2006, was also entered. No Responses/Amendments were filed subsequent to the above Amendment mailed on September 26, 2006.

5. Summary of Claimed Subject Matter

Claim 1 is directed to a method for initializing a SNMP (simple network management protocol) v3 device using an SNMP agent in the SNMPv3 device and an SNMP manager remote

from the SNMPv3 device (Claim 1, preamble).

The subject matter of Claim 1 is described, e.g., at: page 5, line 26 to page 11, line 14. Moreover, the subject matter of Claim 1 involves, e.g.: elements 100, 101, 102, 103, 104, 105, 106, 107, 108, 200, 201, 202, 203, 204, 205, 206, 207, and 208 of FIG. 2.

6. Grounds of Rejection to be Reviewed on Appeal

Claims 1-7 stand rejected under 35 U.S.C. §103(a) as being unpatentable over SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 (hereinafter "Stallings") in view of Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998 (hereinafter "StJohns"). The preceding rejection is presented for review in this Appeal.

Regarding the grouping of the Claims, Claims 2-7 stand or fall with Claim 1, due to their respective dependencies.

7. Argument

A. Introduction

In general, the present invention is directed to a system and method for initializing a Simple Network Management Protocol (SNMP) agent (Applicants' Specification, Title). As disclosed in the Applicants' specification, the present invention is directed to the problem that "[t]he current DOCSIS cable modem system framework, however, does not provide a standard protocol for entering the initial authentication and privacy keys into a cable modem to initialize the cable modem in SNMPv3 mode and vendors must provide proprietary protocols for performing this initialization" (Applicants' specification, p. 2, lines 23-26).

Advantageously, the present invention provides a system and method for initializing an SNMP agent in SNMPv3 mode using a Diffie-Hellman Key exchange protocol for entering the initial authentication and privacy keys into the cable modem (Applicants' specification, p. 4, lines 27-33).

The claims of the pending invention include novel features not shown in the cited references and that have already been pointed out to the Examiner. These features provide advantages over the prior art and dispense with prior art problems such as the absence of a standard protocol for entering the initial authentication and privacy keys into a cable modem to initialize the cable modem in SNMPv3 mode (Applicants' Specification, p. 2, lines 23-26).

It is respectfully asserted that Claim 1 is patentably distinct and non-obvious over the cited references, as will be shown herein below. As such, Claim 1 is presented for review in this appeal.

B. Whether Claim 1 Is Unpatentable Under 35 U.S.C. §103(a) by SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 in view of Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner rejected Claims 1-7 as being unpatentable over SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 (hereinafter "Stallings") in view of Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998 (hereinafter "StJohns"). The Examiner contends that the combination of Stallings and StJohns shows all the elements recited in these claims.

Stallings is directed to a security enhancement for SNMP (Stalling, Title). To that end, Stallings discloses a process referred to as key localization, which is "[t]he process by which a single user key is converted into multiple unique keys, one for each remote SNMP engine" (Stallings, p. 12, col. 2). As is shown in Figure 7 of Stallings, a user password is input to a hash function, which takes a hash of the expanded password string and outputs a user key. Then, for each remote SNMP engine, the user key is input to a hash function that takes a hash of the user key and the remote EngineID of the corresponding remote engine to output a localized key. That is "a single user key is mapped by means of a nonreversible one-way function (i.e., a secure hash function) into different localized keys for different authenticated engines (different agents)" (Stallings, p. 12, col. 2 to p. 13, col. 1). Stallings further discloses that "[a] localized key is defined … as a secret key shared between a user and one authoritative SNMP engine" (Stallings, p. 12).

StJohns is directed to a Diffie-Helman Key Change Management Information Base and Textual Convention (StJohns, Title). To that end, StJohns discloses the following in his Abstract:

> This memo defines an experimental portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a textual convention for doing Diffie-Helman key agreement

key exchanges and a set of objects which extend the usmUserTable to permit the use of a DH key exchange in addition to the key exchange method described in [12].

The KeyChange textual convention described in [12] permits secure key changes, but has the property that if a third-party has knowledge of the original key (e.g. if the agent was manufactured with a standard default key) and could capture all SNMP exchanges, the third-party would know the new key. The Diffie-Helman key change described here limits knowledge of the new key to the agent and the manager making the change.

It will be shown herein below that the limitations of Claim 1 reproduced herein are not shown in Stalling and/or StJohns, and that such Claims should be allowed including those dependent there from as identified in Section 6 herein.

B1. The Cited Combination of Stallings and StJohns Does Not Teach Or Suggest Converting The Shared Secret Into A Readable Password, As Recited In Claim 1

It is respectfully asserted that none of the cited references teach or suggest "converting the shared secret into a readable password", as recited in Claim 1.

The Examiner has cited "Fig 7, element: expended hashed password string; Page 12, Col 1, lines 29-48; human readable password, concatenating and repeating the user's password to itself to generate digest0; generating digest0 from the password; proposal [2]; RFC 2274" as disclosing the preceding limitations of Claim 1. This section is reproduced herein below.

Page 12, col. 1, lines 29-48 of Stalling disclose:

A user requires a 16-octet privacy key and an authentication key of length either 16 or 20 octets. For keys owned by human users, it is desirable that the user be able to employ a human-readable password rather than a bit-string key. Accordingly, RFC 2274 defines an algorithm for mapping from the user password to a 16- or 20-octet key. USM places no restriction on the password itself, but local management policies should dictate that users employ passwords that are not easily guessed.

Password to key generation is performed as follows:

1. Take the user's password as input and produce a string of length 220 octets (1,048,576 octets) by repeating the password value as many times as necessary, truncating the last value f necessary, to form the string digest0. For example, an eight-character password (23 octets) would be concatenated with itself 217 times to form digest0.

2. If a 16-octet key is desired, take the MD5 hash of digest0 to form digest1. If a 20-octet key is desired, take the SHA-1 hash of digest0 to form digest1. The output is the user's key.

The preceding is one portion of the key localization method disclosed in Stallings. The entire key localization method of Stalling is shown in Figure 7 thereof and can be essentially represented by the following sequence: password ->(hash)-> user key ->(hash with remote EngineID)->localized key(s).

However, in the preceding sequence of the key localization method, the shared key is not the user key but is instead the localized key. For example, as explicitly disclosed in Stallings "a localized key is defined ... as a secret key shared between a user and one authoritative SNMP engine" (Stallings, p. 12, col. 2). In view of the preceding, namely that the localized key is the shared secret key, it appears the Examiner has mischaracterized the user key versus the localized key disclosed in Stallings. That is, Stalling discloses converting a readable password into a user key and NOT converting the readable password into the localized key (since the localized key is generated from a hash function applied to the user key and a remote EngineID). Thus, the preceding section of Stallings does not disclose the preceding limitations of Claim 1 recited above.

Moreover, assuming arguendo that the user key is the shared secret, which would be contrary to the explicit disclosure of Stallings which designates the localized key as a shared secret key, then Stallings would still NOT disclose the preceding limitations of Claim 1 recited above. For example, while Claim 1 essentially recites a shared secret converted into a readable password (shared secret -> readable password), Stalling discloses the opposite, namely a readable password converted into a user key (readable password -> user key). Since the claim language recites that the shared secret is converted into a readable password, while Stallings discloses that a readable password is converted into a user key, Stallings does not teach or suggest the preceding limitation, but instead teaches away from it by disclosing the opposite approach.

Thus, neither Stallings nor StJohns, either taken singly or in combination, teach or suggest "converting the shared secret into a readable password", as recited in Claim 1.

Accordingly, Claim 1 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 1 (and, thus, also Claims 2-7) is earnestly requested.

B2. The Cited Combination of Stallings and StJohns Would Change The Principle Of Operation Of Stallings, Thereby Making The Teachings of The Combination Not Sufficient To Render Claim 1 Prima Facie Obvious

MPEP §2143.01 provides, *inter alia*:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary

reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Here, Stalling discloses the generation of a user key, for example, by a user/manager, where the user key is then provided to each remote SNMP engine which hashes the user key with its own remote EngineID to obtain a localized key. That is, in Stallings, the user/manager generates a user key, and the SNMP agent hashes the user key with a remote EngineID to obtain a respective localized key. In contrast, Claim 1 recites the use of the Diffie-Helman key exchange protocol.

Accordingly, each of the entities in Stallings, namely the manager (user key generation side) and the SNMP agent would require a substantial reconstruction and redesign to *possibly* be able to operate as the elements recited in Claim 1. That is, given the different approach disclosed in Stallings versus the claimed invention, each of the entities in Stallings would require a very substantial reconstruction and redesign to be able to implement the Diffie-Helman key exchange protocol in accordance with Claim 1 .

Moreover, the principle of operation of Stallings is essentially disclosed therein as follows: "a single user key is mapped by means of a nonreversible one-way function (i.e., a secure hash function) into different localized keys for different authentication engines (different agents)" (Stallings, p. 12, col. 2 to p. 13, col. 1). However, the application of the Diffie-Helman key exchange protocol to the teachings of Stallings would completely obviate the need for the nonreversible one-way secure hash function, as well as the mapping of a single user key into different localized keys, thereby changing the principle of operation of the key localization

method disclosed in Stallings. Thus, Stallings is improperly applied to the pending Claims per MPEP §2143.01 and, thus, the teachings of the combination of Stallings and StJohns is not sufficient to render the claims prima facie obvious.

Accordingly, Claim 1 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 1 (and, thus, also Claims 2-7) is earnestly requested.

B3. No Teaching, Suggestion, or Motivation Exists To Combine And/Or Modify Stallings And/Or StJohns To Produce The Invention Claimed In Claim 1

"Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so" (MPEP §2143.01, citing *In re Kahn*, 441 F.3d 977, 986 78 USPQ2d 1329, 1335 (Fed. Cir. 2006)).

Here it is respectfully asserted that no such teaching, suggestion, or motivation exists to combine and/or modify the references to produce the invention claimed in Claim 1.

For example, in specifying a rationale for combining and modifying the references, the Examiner has stated "[a]t the time of the invention, it would have been obvious to a person of ordinary skill in art to combine the teachings of StJohns with Stallings to utilize a Diffie-Hellman key exchange protocol for managing/updating keys in order to provide stronger key security (please see Page 1, StJohns), and which might consequently eliminate the need for using key localization" (Office Action, p. 6).

However, Stallings has already provided a stand-alone and complete solution directed to

the requirement for the use of authentication and privacy services of SNMPv3, namely that, for any communication between a principal on a non-authoritative engine and a remote authoritative engine, a secret authentication key and a secret privacy key must be shared (Stallings, p. 11, lines 54-58). Given the security provided by the technique disclosed in Stallings, which relies upon "a nonreversible one-way function (i.e., a secure hash function)" (Stallings, p. 12, lines 65-67), there is no NEED WHATSOEVER, let alone any teaching, suggestion, or motivation, to modify Stallings with the use of the Diffie-Hellman Key Exchange disclosed by StJohns as proposed by the Examiner.

Regarding the Examiner statement that stronger key security is provided by the combination, the Court of Appeals for the Federal Circuit has "emphasized that the proper inquiry is 'whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination,' not whether there is something in the prior art as a whole to suggest that the combination is the most desirable combination available" MPEP §2143.01 citing In re Fulton, 391 F.3d 1195, 1200-01, 73 USPQ2d 1141, 1145-46 (Fed. Cir. 2004).

Thus, as argued above, no teaching, suggestion, or motivation exists to modify the combined and/or modify the references to obtain the invention claimed in Claim 1, thus rendering the combination and/or modification of Stallings and StJohns improper.

Accordingly, Claim 1 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 1 (and, thus, also Claims 2-7) is earnestly requested.

C. Conclusion

At least the above-identified limitations of the pending claims are not disclosed or suggested by the teachings of Stallings and/or StJohns. Accordingly, it is respectfully requested that the Board reverse the rejection of Claim 1-7 under 35 U.S.C. §103(a).

Please charge the amount of $500.00, covering fee associated with the filing of the Appeal Brief, to **Thomson Licensing Inc., Deposit Account No. 07-0832**. In the event of any non-payment or improper payment of a required fee, the Commissioner is authorized to charge **Deposit Account No. 07-0832** as required to correct the error.

Respectfully submitted,

BY: /Guy H. Eriksen/
Guy H. Eriksen, Attorney for Applicants
Registration No.: 41,736
Telephone No.: (609) 734-6807

December 7, 2006

Thomson Licensing Inc.
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

8. CLAIMS APPENDIX

1. (Previously Presented) A method for initializing a SNMP (simple network management protocol) v3 device using an SNMP agent in the SNMPv3 device and an SNMP manager remote from the SNMPv3 device, comprising:

utilizing a Diffie-Hellman key exchange protocol by the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device,

wherein said utilizing step includes:

generating an associated random number and public value by both the SNMP manager and the SNMP agent;

passing the public value of the SNMP manager to the SNMP agent in a configuration file;

reading, by the SNMP manager, the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent;

computing a shared secret, by the SNMP agent and the SNMP manager, using the Diffie-Hellman key exchange protocol;

converting the shared secret into a readable password;

converting the readable password into a secret key; and

setting the initial authentication key and the initial privacy key to the value of the secret key.

2. (Original) The method of claim 1, wherein the readable password comprises a 16

character password.

3. (Original) The method of claim 1, wherein the secret key comprises a 16 byte string.

4. (Original) The method of claim 1, further characterized in that the configuration file comprises a proprietary configuration file element for passing the public value of the SNMP manager to the SNMP agent.

5. (Original) The method of claim 4, wherein the SNMPv3 device operates in a SNMPv1/v2c enabled network comprising a SNMPv2c device, and wherein the proprietary configuration file element is ignored by the SNMPv2c device.

6. (Previously Presented) The method of claim 1, wherein the public value of the SNMP manager is included in a management information base (MIB) object in the configuration file.

7. (Previously Presented) The method of claim 1, wherein the public value of the SNMP manager is initially stored in a third entity different from that associated with the SNMP manager and the SNMP agent, and the method comprises downloading the configuration from the third entity by the SNMP agent.

9. RELATED EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None